Program verification

Big area in practice (google, meta, ...). All sorts of fancy logics, important one: separation logic.
For this course: the foundation for all program logic:

HOARE LOGIC : examples, proof rules, theoretical results (relative completness)

{} precondition ☆ assertions

```
y := 0
z := 1
while y ≠ x do
    y := y+1 ;
    z := z*y ;
```
W

{z = x!} postcondition, if the program terminates, then z = x! Zato za precondition ne rabimo {x≥0}

Hoare logic is compositional - the proof rules follow the syntactic structure of the program.

$$\frac{\{\phi\}\, C_1\, \{\theta\} \qquad \{\theta\}\, C_2\, \{\psi\}}{\{\phi\}\, C_1 ; C_2\, \{\psi\}}$$

$$\frac{\{\eta\}\, c\, \{\eta\}}{\{\eta\}\ \text{while } B \text{ do } C\ \{\eta \wedge \neg B\}}$$

; η is called the INVARIANT

Consequence rule:

$$\frac{\{\phi'\}\, C\, \{\psi'\}}{\{\phi\}\, C\, \{\psi'\}}$$

SIDE CONDITIONS $(\phi \to \phi')\ (\psi' \to \psi')$

Assignment:

$$\frac{}{\{\psi[e/x]\}\ x := e\ \{\psi\}}$$

☆
$$\frac{\{z*(y+1) = (y+1)!,\ y+1 \neq 0\}\ y := y+1\ \{z*y = y!,\ y \neq 0\}}{\{z = y!,\ y \neq 0,\ y \neq x\}\ y := y+1\ \{z*y = y!,\ y \neq 0\} \qquad \{z*y = y!,\ y \neq 0\}\ z := z*y\ \{z = y!,\ y \neq 0\}}$$

$$\frac{\{z = y!,\ y \neq 0,\ y \neq x\}\ y := y+1\ ;\ z := z*y\ \{z = y!,\ y \neq 0\}}{\{z = y! \wedge y \neq 0\}\ W\ \{z = y! \wedge y \neq 0 \wedge y = x\}}$$ ☆

$$\frac{\{\}\, y := 0 ;\ z := 1\, \{y = 0 \wedge z = 1\} \qquad \{y = 0 \wedge z = 1\}\ W\ \{z = x!\}}{\{\}\, y := 0 ;\ z := 1,\ W\ \{z = x!\}}$$

☆ $y = 0 \wedge z = 1 \to z = y! \wedge y \neq 0$ ✓✓

$z = y! \wedge y \neq 0 \wedge y = x \to z = x!$ ✓✓

} side conditions

Prosojnice ☆ $z = y! \wedge y \neq 0 \wedge y \neq x \to z*(y+1) = (y+1)! \wedge y+1 \neq 0$